Приложение № 2
към рамков договор № 67/24.10.2024 г. (ПО-16-3173/24.10.2024 г.)

ЗАЯВКА по Рамков договор № 67/24.10.2024 г. (ПО-16-3173/24.10.2024 г.) от 2024 г.		☐
ЗАЯВКА (актуализирана)		☑ [1]
Позиция от ПГ-2024 г.:	*№ по ред от ПГ*	*2*
Описание на дейност/проект съгласно ПГ:	*Доставка на хардуерни и софтуерни ресурси за надграждане на инфраструктурата на МЕ*	
CPV код	*48820000-2*	
Изискване за достъп до класифицирана информация ДА/НЕ	*НЕ*	
Стойност: (*стойността следва да съответства на заложената в План-графика***) без ДДС**, *в т.ч. разбивка на стойността за проекти на части/ с акредитив/ авансово*		*486 840,00 лв. без ДДС*
Начин за плащане: *(еднократно, на части, периодично, авансово или др.)*		*Еднократно след подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка*
Плащане с акредитив или авансово ДА/НЕ		*НЕ*
Документи за плащане с акредитив или авансово		*неприложимо*
Срок на изпълнение: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**		*За доставка на оборудването до 27.12.2024 г.*
Гаранционен срок: (*от дата – до дата или в месеци, ако не е обвързан с конкретна дата***)**		*Съгласно Техническа спецификация*
Отчитане: *(периодично – посочва се период, еднократно, срок за отчитане, отчетни документи)*		*С подписване на приемо-предавателен протокол по чл. 6 от договора, удостоверяващ приемане на извършената доставка.*
Приложения: (*напр: технически параметри, образци на отчетни документи*)		*Техническа спецификация*
Настоящата заявка да се изпълни при условията на приложените Технически параметри.		
ЗАЯВКАТА е ИЗГОТВЕНА И СЪГЛАСУВАНА ОТ:		
Координатор по заявката:		*Подпис:*
Ръководител на проект/дейност по заявката (напр: представител на дирекцията – Заявител):		
ЗАЯВКАТА е ОДОБРЕНА ОТ:		
Ръководител на договора от страна на ВЪЗЛОЖИТЕЛЯ:		
ЗАЯВКАТА е ПРИЕТА ЗА ИЗПЪЛНЕНИЕ ОТ ИЗПЪЛНИТЕЛЯ:		

[1] Отбелязва се в случай че заявката е актуализирана

Координатор от „Информационно обслужване“ АД по заявката		*Подпис:*
Ръководител на проект/дейност по заявката		*Подпис:*
Ръководител по изпълнението на Договора от „Информационно обслужване“ АД		*Подпис:*

Заличаванията в документите са на основание чл. 4 от Общия регламент относно защитата на данните - Регламент (ЕС) 2016/679

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

ЗА

ДОСТАВКА НА НА ХАРДУЕРНИ И СОФТУЕРНИ РЕСУРСИ ЗА НАДГРАЖДАНЕ НА ИНФРАСТРУКТУРАТА НА МИНИСТЕРСТВО НА ЕНЕРГЕТИКАТА

I. ПРЕДМЕТ

В предмета на заявката се включват следните дейности:

1. Доставка на хардуерни и софтуерни ресурси за нуждите на Министерство на енергетиката (МЕ) (наричано по-нататък за краткост „оборудването“), подробно описано по вид, количество и технически характеристики в настоящата Техническа спецификация.
2. Гаранционно обслужване на доставеното по т. 1 оборудване, осигурено в рамките на срока на гаранционно обслужване в съответствие с предписанията на производителя.

Изискванията на Възложителя относно обхвата и изпълнението на дейностите по доставка на хардуерни и софтуерни ресурси за надграждане на инфраструктурата на МЕ са както следва:

1. Специализиран дисков масив за резервни копия

Спецификация – минимални изисквания	
REQ.1.	Тип на шасито – за вграждане в 19-инчов шкаф.
REQ.2.	Количество – 1 брой
REQ.3.	Капацитет – минимум 32TB използваем капацитет преди комепресия и дедупликация, с възможност за бъдещи разширения до 170TB.
REQ.4.	Устройството трябва да разполага с мин. 4 порта със скорост 10 Gb/s със съответните SFP модули и 2 порта на 16Gb/s със съответните SFP модули.
REQ.5.	Основни функционални изисквания: - Данните да могат да се изпращат по LAN, като се използват CIFS, NFS, NDMP протоколи. - Да поддържа изпращане на данните през SAN/FC (Storage Area Network/Fibre Channel), чрез добавяне само на комуникационни модули - Всички гореизброени методи за комуникация да могат да работят едновременно.
REQ.6.	Устройството/системата трябва да поддържа Inline дедупликация на данните.
REQ.7.	Устройството/системата трябва да поддържа употребата на софтуерни приставки (plug-ins) на backup сървъра/медия сървъра/storage устройството/backup клиента, които да позволяват дедупликация на данните преди изпращането им към backup устройството.
REQ.8.	Производителността да е поне 12 TB/hr.
REQ.9.	Устройството трябва да поддържа криптиране при репликация.
REQ.10.	Устройството трябва да поддържа репликация на дедуплицираните данни към същия или подобен тип устройство.

Спецификация – минимални изисквания	
REQ.11.	Устройството трябва да поддържа архивиране (backup) на данните с възможност за заключване на архивираните файлове (retention lock) включително с възможност за допълнително активиране на функционалността съобразно нуждите на Възложителя (не е предмет на настоящата заявка).
REQ.12.	Устройството трябва да поддържа моментни копия/snapshots.
REQ.13.	Устройството да поддържа виртуална лентова библиотека.
REQ.14.	Устройството да поддържа глобална дедупликация на всички пространства (CIFS/NFS shares, VTL, различни директории и др.).
REQ.15.	Гаранция - 36 месеца

2. **Защита на електронна поща – 2-ри слой**

Спецификация – минимални изисквания	
	Тип решение: 2 броя хардуер (High-Availability) с вграден софтуер и минимум 3-годишна поддръжка, както и минимум 3-годишен абонамент за прилежащи услуги към хардуерните устройства за 200 потребителя
REQ.1.	Решението трябва да може да открива и идентифицира зловреден код, който е скрит и влиза в организацията чрез електронната поща, като трябва да се използват технологии и методи за засичане, които да не са базирани само на статичен анализ чрез дефиниции, статични списъци или правила, а да може да извършва и динамичен анализ и да открива непознати "zero-day" заплахи.
REQ.2.	Решението трябва да се предоставя под формата на специализиран хардуер, като производителят трябва да е отговорен и да предостави лицензи за софтуер за поне 120 виртуални машини за анализ, с прилежащите им операционни системи и приложения.
REQ.3.	Решението трябва да притежава следните сертификати: Federal Information Processing Standards (FIPS) 140-2 и Common Criteria (CC).
REQ.4.	Решението трябва да може да открива фишинг и spear-фишинг атаки. Трябва да може да анализира прикачени файлове и URL адреси в електронните съобщения, за да открива опити за компрометиране на системите на организацията.
REQ.5.	Решението трябва да може да открива impersonation атаки (представяне с чужда самоличност). Трябва да се позволява конфигурирането на отношения между имена и email адреси, така че да се засичат опити за impersonation атаки, които копират имената или email адресите на потребителите.
REQ.6.	Решението трябва да може да засича зловреден код с голяма точност, с изключително малък процент на грешни показания. Трябва да може да се открива с точност зловреден код, независимо от MIME тип, тип на разширение (extension) и независимо дали са използвани техники за скриване или архивиране на съдържанието на електронните съобщения.
REQ.7.	Решението трябва да може да поставя в карантина email съобщения, които съдържат URL адреси в тялото си, съдържат MS Office документи, PDF документи, архиви и HTML файлове, замаскирани JAVA скриптове, замаскирани, съкратени или пренасочващи URL адреси.
REQ.8.	Решението трябва да може да разпознава заплахи като извършва локален анализ, без да е необходимо да изпраща файлове, проби от зловреден код или изпълним код извън организацията или към облачно-базирани платформи за анализ.
REQ.9.	Решението трябва да може да анализира множество типове файлове, използвайки различни приложения и техни версии за анализа, съответно за разширения

	(минимално): exe, dll, pdf, pub, doc, docx, xls, xlsx, js, gif, jpeg, png, tiff, swf, eml, mov, qt, mp4, jpg, mp3, asf, ico, htm, hta, url, rm, com, vcf, ppt, rtf, chm, hlp.
REQ.10	Решението трябва да може да извлича и анализира вмъкнати файлове в документи, като например pdf, rtf или MS Office документи.
REQ.11	Решението трябва да може да поставя в карантина и да алармира за криптирани MS Office документи.
REQ.12	Решението трябва да може да поставя в карантина и да алармира за прикачени MS Office документи, които съдържат макроси или имат вградени в тях документи, независимо от резултата от анализа.
REQ.13	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат в себе си съкратени URL адреси.
REQ.14	За електронни съобщения, които съдържат URL адреси, които водят до сваляне на файлове, решението трябва да може да извлича и анализира въпросните файлове от URL адресите, като да може да се блокира съобщението, ако файловете се окажат зловредни.
REQ.15	Решението трябва да може да поставя в карантина и да алармира за електронни съобщения, които съдържат прикачени JAR файлове или съдържат URL адреси, които водят до JAR файлове.
REQ.16	Решението трябва да може да извлича и анализира URL адреси от съдържанието на електронните съобщения и от секцията „Относно“ на съобщенията, както и от прикачени PDF или MS Office документи.
REQ.17	Решението трябва да може да засича следните техники, които се използват от атакуващите хакери, за да подмамят потребителите да достъпят конкретни URL адреси: заместване на знак от адреса с друг (typosquatting), използване на линк към различен адрес от изобразения (URL overlay).
REQ.18	Решението трябва да може да анализира URL адреси от тип ftp, http и https.
REQ.19	Решението трябва да може да анализира base64 кодирани URL адреси.
REQ.20	Решението трябва да анализира прикачени архиви тип 7Z, ZIP, LZH, RAR. Ако архивите са защитени с парола, решението да може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение, в самите файлове-архиви или в прикачени изображения към съобщението чрез OCR технология.
REQ.21	Решението трябва да може да извлича и анализира URL адреси от заключени с парола PDF или MS Office документи. Решението да може автоматично да търси подходящи варианти за парола в съдържанието на електронното съобщение или в прикачени изображения към съобщението чрез OCR технология (изображения тип JPEG, PNG, BMP, TIFF).
REQ.22	Решението трябва да може да анализира файлове не само чрез статичен анализ с дефиниции, но и чрез алгоритми за машинно обучение и динамичен анализ тип sandbox.
REQ.23	Решението трябва да може да анализира (във виртуалните машини за динамичен анализ) свалените файлове от заявки, идващи от exploit атаки. Например, ако прикачен файл към електронно съобщение съдържа скрипт / макрос, който опитва да свали допълнителни файлове и съдържание, то решението трябва да може успешно да ги свали и анализира, за да се открият и предотвратят атаки, които се развиват на няколко фази.
REQ.24	Решението трябва да може да открива с много висока точност, с възможно най-малко грешни показания, файлове, които след анализ на поведението се държат по подобие на зловреден код: поведение, което опитва да избегне засичане, инсталиране на нежелани програми, промени по системните настройки, намаляване на цялостната производителност на системата, потенциално нежелани програми (PUP), потенциално нежелани приложения (PUA), adware процеси, инструменти, които често се използват от атакуващи хакери.

REQ.25	По време на анализа във виртуалните машини решението трябва да може да извлича и анализира URL адресите в паметта на машините.
REQ.26	Решението трябва да може да засича ransomware криптиращи атаки и атаки, предназначени за POS терминали.
REQ.27	Решението трябва да може да алармира за зловредни процеси (файлове и URL адреси), които не са били засечени в първоначалните 24 часа, а на по-късен етап е установено, че са зловредни.
REQ.28	Решението трябва да предоставя цялостна информация след анализ на зловреден код. Информацията трябва да включва използвани уеб линкове за атаката, хеш суми на свалените файлове, цялостен одит на действията по системите (променени ключове от регистрите, създаване и изпълнение на файлове, промяна в автоматичните настройки и параметрите за стартиране на приложения), както и да се предоставя информация за хронологичния ред от събития, свързани с атаката, започващи от фазата на уеб-експлоатация и първоначално проникване, до свалянето на код, установяване на контрол над системите и опитите за извличане на данни извън организацията.
REQ.29	Решението трябва да предоставя следствена информация след динамичния анализ на файлове, представена в графичен вид, изобразявайки процеси, достъпи до паметта, промени по файлове и регистри, качени DLL библиотеки, инжектиране на код, heap spraying процеси, mutex процеси.
REQ.30	Решението трябва да може да предоставя, където е възможно, информация за атакуващата хакерска групировка и възможни стъпки за отстраняване на щетите (remediation) след дадена атака.
REQ.31	Ако при анализ на зловреден прикачен файл се установят опити за мрежови свързвания извън организацията от него, решението трябва да сигнализира и за тях при вдигането на съответната аларма.
REQ.32	Решението трябва да може да предоставя screenshot на зареден в браузър зловреден URL адрес по време на анализа му, за да се добие визуална представа за съдържанието на URL адреса.
REQ.33	Решението трябва да може да прави корелация на електронни съобщения със сходни характеристики, като например с еднакви прикачени файлове, еднакви заглавни части, еднакви изпращачи и т.н. и да може да ги групира като email кампании.
REQ.34	Решението трябва да може да прави анализ на входящи електронни съобщения, използвайки едновременно множество виртуални машини с различни операционни системи, като например минимално Windows 7 или Mac OSX, с различни версии на Service Pack, на 32 и на 64 битови платформи.
REQ.35	Решението не трябва да използва комерсиален хипервайзор, който да може да бъде засечен и избегнат от зловредния код, като например VMware, Hyper-V, KMV, Citrix и т.н.
REQ.36	Решението трябва да използва собствен, специално изграден хипервайзор.
REQ.37	Решението трябва да позволява промяна на настройките на виртуалните машини, на които ще се извършва динамичният анализ. Администраторите трябва да могат да променят поне следните параметри: използвани потребителско име, домейн, име на работната станция, историята от браузването, използваният Outlook акаунт, езика на машината, времевата зона на машината.
REQ.38	Решението трябва да може да се справя с техники за избягване от засичане (evasion techniques), например използване на ping команди, проверка на домейн, проверка на отметки в наличните браузъри.
REQ.39	Email решението трябва да поддържа inline MTA режим на работа.
REQ.40	Email решението трябва да поддържа SPAN/TAP режим на работа.
REQ.41	Email решението трябва да поддържа BCC режим на работа.

REQ.42	Решението трябва да позволява (по избор от администратор) извършване на динамичен анализ на файлове във виртуалните машини, както в режим на изолация (без да е необходима свързаност с Интернет), така и с позволено мрежово свързване от виртуалните машини, за да се добие цялостен анализ на зловредния код.
REQ.43	Решението трябва да използва специално заделен мрежови интерфейс, когато е пуснато в „жив“ режим, за да се избегне допускането на зловреден мрежови трафик към реалната вътрешна мрежа на организацията; Мрежовият интерфейс трябва да позволява на зловредния код да достъпва външни хакерски командни сървъри и да сваля всички допълнителни модули и артефакти, които са му необходими, за да се изпълни изцяло за анализ.
REQ.44	Решението трябва да може да симулира потребителски действия, за да изпълни зловреден код изискващ подобни действия, като например щракане с мишката или конфигуриране на конкретни данни.
REQ.45	Цялостният анализ на електронно съобщение не трябва да отнема повече от 10 минути.
REQ.46	Решението трябва да позволява на администраторите да конфигурират максималното време за анализ на електронните съобщения.
REQ.47	Решението трябва да позволява използването на YARA правила и да позволява конфигурирането на автоматични аларми или поставяне в карантина, ако дадено съобщение отговаря на зададените YARA правила.
REQ.48	Решението трябва да може да засича и отчита опити за мрежова комуникация с Интернет от виртуалните машини по време на анализа.
REQ.49	Решението трябва да позволява на администраторите да посочват и обвързват с кои приложения да се стартират различните файлови разширения по време на анализа във виртуалните машини.
REQ.50	Решението трябва да може да се имплементира в различни режими, както „Inline”, на пътя на трафика, с възможност за блокиране, така и „Out-Of-Band“, където да се анализират копия на електронните съобщения.
REQ.51	Решението трябва да може да изпраща автоматични известия чрез Syslog, HTTP, SNMP и SMTP протоколи.
REQ.52	Решението трябва да поддържа криптирана TLS комуникация (opportunistic или imposed), за да се запази конфиденциалността на електронните съобщения.
REQ.53	Решението трябва да може да изпраща автоматични известия когато блокира или постави в карантина дадено електронно email съобщение.
REQ.54	Решението трябва да позволява конфигурирането на обема на заделеното място за карантина на съобщенията и да може да изпраща автоматични известия когато заделеното пространство се запълни до определен процент.
REQ.55	Решението трябва да позволява използването на прокси с оторизация за свързване със сървър за обновления на софтуера и информацията за нови заплахи.
REQ.56	Решението трябва да позволява администрация чрез уеб-базирана конзола, без да се изисква инсталирането на допълнителен софтуер за достъпването ѝ.
REQ.57	Решението трябва да позволява конфигурирането на ACL списъци, за да се ограничи достъпа до интерфейса за централизирано управление.
REQ.58	Решението трябва да използва криптирана комуникация между администраторите и конзолата за централизирано управление. Трябва да позволява вмъкването на собствени дигитални сертификати на организацията.
REQ.59	Решението трябва да позволява локално конфигуриране или чрез синхронизация с NTP сървър на използваните време и часова зона.
REQ.60	Решението трябва да поддържа ролево-базиран достъп до конзолата за управление. Да могат да се задават различни профили и права (администратор, оператор, одитор и т.н.),

	като се задава кои отчети, аларми и информация могат да виждат в конзолата за управление.
REQ.61	Решението трябва да поддържа LDAP, TACACS + или RADIUS методи за вписване на потребителите.
REQ.62	Решението трябва да може да изпраща известия за собственото си здраве и процеси и генерираните отчети, чрез SMTP, SNMP и Syslog протоколи.
REQ.63	Решението трябва да позволява извличането на аларми и отчети за активност на зловреден код в PDF формат.
REQ.64	Решението трябва да позволява групирането на аларми за зловредни email съобщения по поне следните критерии: по изпращачи, по получатели, по видове вдигнати аларми, по email кампания.
REQ.65	Решението трябва да позволява генерирането на отчети в PDF или в CSV формат, според типа информация в тях: вдигнати аларми и техните детайли, тип инфекция, обобщителна информация за предоставяне пред ръководните органи на организацията, списък с достъпените сървъри при callback комуникация и други.
REQ.66	Решението трябва да предоставя опция да получава и изпраща обекти за анализ, когато бъде достигнат зададен лимит на капацитета на обработваните обекти от решението, към предварително зададен локално разположен клъстър или към специализирани хардуерни устройства за балансиране на производителността.
REQ.67	Решението трябва да позволява извличането на метаданни от email съобщенията, минимално получател, прикачени файлове и вмъкнати URL адреси, като тези метаданни да могат да се изпращат към решение тип SIEM, чрез HTTP или чрез Rsyslog протокол.
REQ.68	Устройството да може да анализира до 600 уникални прикачени файлове към email съобщения в час
REQ.69	Устройството да може да анализира прикачени файлове и URL адреси в email съобщенията за 600 потребителя
REQ.70	Устройството да е с максимална големина 1RU
REQ.71	Устройството да разполага минимално със следните портове за наблюдение на мрежата: 2x 1GigE BaseT
REQ.72	Допълнителни портове: 2x 1GigE BaseT портове за управление, сериен порт, 4x Type A USB, IPMI, VGA
REQ.73	Резервирано захранване – 1+1
Гаранция и поддръжка:	
REQ.74	Хардуерната гаранция за срок от минимум 3 (три) години.
REQ.75	Техническа поддръжка за срок от минимум 3 (три) години.
REQ.76	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.
REQ.77	Обновяване на дефиниции и сигнатури за срок от минимум 3 (три) години

3. **Комутатор сървърен достъп**

Спецификация – минимални изисквания	
REQ.1.	Количество – 1 брой
REQ.2.	Тип на кутията/шасито - за монтаж в 19“ шкаф
REQ.3.	Захранване – модулно, с минимум два токозахранващи модула за резервиране, 220-240v AC, 50Hz
REQ.4.	Модулни вентилатори
REQ.5.	Минимум 24 порта поддържащи 1000 Base-T интерфейса

Спецификация – минимални изисквания	
REQ.6.	Да притежава минимум 8 порта поддържащи 1GE и 10GE чрез допълнителен външен модули
REQ.7.	Брой USB портове - минимум 1
REQ.8.	Да поддържа изолиране на потребителите от един и същ VLAN
REQ.9.	Да поддържа 802.1X на всички портове
REQ.10.	Да поддържа 802.1X идентификация и оторизация с прилагането на динамични VLAN и ACL.
REQ.11.	Да поддържа идентификация на база MAC адреси
REQ.12.	Да поддържа идентификация чрез вграден Web портал
REQ.13.	Да поддържа комбиниране на методите идентификация на един порт – 802.1x, MAC адрес, WEB идентификация.
REQ.14.	Да поддържа RADIUS CoA
REQ.15.	Да поддържа хардуерно реализирани листи за филтриране на трафика на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове
REQ.16.	Да поддържа 802.1AE 256 битово криптиране на всички портове
REQ.17.	Да поддържа автоматично инспектиране на DHCP трафика със следните функции: · блокиране на DHCP заявки с разлика в MAC адреса на Ethernet фрейма и MAC адреса в DHCP заявката. · блокиране на DHCP пакети за освобождаване на адрес или отказ, които идват от порт различен от този, през който е получен IP адреса. · Защита от IP Spoofing
REQ.18.	Да поддържа автоматично запаметяване на използвания от клиентското у-во MAC адрес и да блокира мрежовия достъп за други устройства свързвани към същия порт
REQ.19.	Да поддържа игнориране на BPDU пакети получавани от клиентски портове
REQ.20.	Да подържа възможност за игнориране на STP root bridge информация през неоторизирани портове
REQ.21.	Да поддържа криптографски метод за проверка на автентичността на използвания софтуер
REQ.22.	Хардуерно маршуритизиране за IPv4 и IPv6 със следните параметри, като минимум: · Производителност - 200Gbps · Forwarding – 150Mpps · Брой IPv4 и IPv6 маршрута – 48000 · Multicast маршрути - 8000 · SVI интерфейси - 1000 · Пакетни буфери – 16MB
REQ.23.	DRAM - минимум 8GB DRAM
REQ.24.	Да поддържа стекове свързване между минимум осем устройства чрез използване на стак портове с капацитет от 480Gbit
REQ.25.	Да поддържа Statefull Switch Over (SSO) между комутатори в един стек за минимум следните функции: · Маршрутизиране · STP · 802.3ad
REQ.26.	MAC адреси – минимум 32000

Спецификация – минимални изисквания	
REQ.27.	Да поддържа Jumbo frames от поне 9198 байта
REQ.28.	Да поддържа минимум 4000 802.1Q VLAN
REQ.29.	Да поддържа енкапсулация на трафика във VXLAN
REQ.30.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1w
REQ.31.	Да поддържа следните протоколи за маршрутизация: · Статично маршрутизиране за IPv4 и IPv6 · RIPv1, RIPv2, RIP-NG · OSPFv2 и OSPFv3 · BGPv4 · IS-ISv4 · IGMPv2 и IGMPv3 snooping · Мултикас маршрутизиране с PIM-SM и PIM-SSM · Маршрутизиране на база политики · Виртуализация на машрутизиращите таблици и протоколи · VRRP
REQ.32.	Да поддържа IEEE 802.3ad LACP протокол
REQ.33.	Да поддържа IEEE 802.3ad групи с портове от различни комутатори в един стек
REQ.34.	Да поддържа LLDP
REQ.35.	Да поддържа класифициране на трафичните потоци на ниво апликациите посредством вградена DPI система
REQ.36.	Да поддържа QoS със следните функции, като минимум: · Минимум 8 изходящи пакетни опашки на всеки порт. · Групиране на трафика в трафични класове на база произволни комбинации от Layer2, Layer 3, Layer 4 и Layer 7 трафични параметри, 802.1p и DCSP маркировка · Traffic policing на база трафични класове · Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR PIR и Commited Burst параметри. · Traffic shaping на база трафични класове · Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всяка опашка, като процент от пропускателната способност на интерфейса · Управление на пакетните опашки чрез задаване на минимално гарантирана скорост за всяка опашка. · Поддръжка на приоритетна опашка (PQ) · Поддръжка на Weighted Tail Drop (WTD) алгоритъм за предотвратяване на задръствания · DSCP и 802.1p маркиране и премаркиране на трафика на база трафични политики
REQ.37.	Да поддържа MPLS
REQ.38.	Да поддържа L2 и L3 MPLS VPN
REQ.39.	Да поддържа BGP EVPN
REQ.40.	Да поддържа работа като Multicast DNS шлюз
REQ.41.	Да поддържа изграждането на софтуерно управлявани виртуални мрежи (SDN Overlays)
REQ.42.	Да поддържа изграждането на SDN Overlay с използване на BGP EVPN, MPLS, LISP или подобен контролен протокол

Спецификация – минимални изисквания	
REQ.43.	Да поддържа динамична сегментация на потребителите на база минимум MAC адреси, профилиране на потребителското устройства и 802.1x удостоверяване на идентичност
REQ.44.	Да поддържа минимум следните методи за управление и наблюдение: · Управление чрез конзола и GUI · RMON. · IPv4/v6 ping · DNS · TFTP · FTP · NTP клиент и сървър · SSHv2 и SNMPv3 · Експортиране на трафична информация за минимум 64000 трафични потока чрез IPFIX, Netflow, JFlow или подобен протокол към външна система за трафичен анализ · Конфигурация в отделен конфигурационен файл, който позволява бързо и лесно преместване на конфигурацията върху ново у-во · Задаване ниво на достъп до системата за всеки администратор. · Работа с външна система за съхраняване на изпълнените от всеки администратор команди · Traffic policing за контролиране на трафика до контролната система на комутатора · Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. · Отделен Ethernet порт за out of band управление и наблюдение на устройството · Да поддържа NETCONF/YANG интерфейс · Да поддържа възможност за работа с контейнери · Да поддържа увеличаване на обема за съхранение на данни чрез включване на външен USB диск през минимум един USB 3.0 интерфейс · Да поддържа стрийминг на телеметрия на база YANG моделите
REQ.45.	Устройството да е окомплектовано със съответните лицензи и права за използване според условията на производителя
REQ.46.	Устройството да е окомплектовано с необходимите планки за монтаж в 19“ шкаф, стекови модули, външни интерфейсни модули и кабели.
Гаранция и поддръжка:	
REQ.47.	Срок на хардуерната гаранция - минимум 3 (три) години.
REQ.48.	Срок на техническа поддръжка – минимум 3 (три) години.
REQ.49.	Получаване на нови версии на софтуера - минимум 3 (три) години.

4. **Комутатори за достъп – тип 1**

Спецификация – минимални изисквания	
REQ. 1.	Количество – 6 броя.
REQ. 2.	Монтаж - в 19“ шкаф.

REQ. 3.	Токозахранване – модулно, с два токозахранващи модула, AC.
REQ. 4.	48 порта 1GE RJ45 с поддръжка на PoE+ и 4 порта 10GE SFP модули.
REQ. 5.	Вграден хардуерен порт за стеково свързване с производителност 80Gbps.
REQ. 6.	Изграждане на стек от 8 комутатора.
REQ. 7.	Брой USB портове – 1.
REQ. 8.	Сериен конзолен порт – 1.
REQ. 9.	Изолиране на потребителите от един и същ VLAN.
REQ. 10.	Идентификация и оторизация на достъпа: 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL. MAC authentication bypass. Идентификация чрез вграден Web портал. Комбиниране на методите за идентификация на един порт – 802.1x, MAC адрес, WEB идентификация. RADIUS CoA. 802.1x идентификация на повече от едно устройство на комутаторен порт. 802.1x Multi-Domain идентификация.
REQ. 11.	Хардуерно реализирани листи за филтриране на трафика, на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове.
REQ. 12.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ. 13.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ. 14.	802.1AE с 128 битово криптиране, с MKA.
REQ. 15.	DHCP Snooping или еквивалентен метод.
REQ. 16.	DHCP опция 82.
REQ. 17.	Dynamic ARP inspection или еквивалентен метод.
REQ. 18.	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ. 19.	Автоматично запаметяване на използвания от първото клиентското у-во MAC адрес и блокиране на мрежовия достъп за други устройства, които се свързват към същия порт.
REQ. 20.	Spanning Tree защити - BPDU Guard и Root Guard.
REQ. 21.	Хардуерен модул за удостоверяване автентичността на хардуерна и софтуера чрез използване на криптографски методи.
REQ. 22.	Хардуерно IP forwarding и комутиране със следните параметри: Производителност – 175 Gbps. Forwarding – 130 Mpps. MAC адреси – 16000. IPv4 маршрути – 3000.

	Multicast маршрути – 1000. SVI интерфейси – 512. Пакетни буфери – 6MB.
REQ. 23.	DRAM - 2GB.
REQ. 24.	Statefull Switch Over (SSO) между комутатори в един стек за следните функции: Рутиране. STP. 802.3ad.
REQ. 25.	Jumbo frames - 9198 байта.
REQ. 26.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ. 27.	Функция Private VLAN.
REQ. 28.	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ. 29.	Рутинг протоколи: RIP OSPF с 1000 маршрута. Мултикас рутиране с PIM. Рутиране на база политики. VRRP
REQ. 30.	IEEE 802.3ad LACP протокол.
REQ. 31.	IEEE 802.3ad групи с портове от различни комутатори в един стек.
REQ. 32.	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ. 33.	QoS със следните функции, като минимум: HQoS. 8 изходящи пакетни опашки на всеки порт. Групиране на трафика в трафични класове на база Layer2, Layer 3 и Layer 4 трафични параметри, 802.1p и DCSP маркировка. Traffic policing. Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR PIR и burst параметри. Traffic shaping. Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. Поддръжка на две приоритетни опашки (PQ) на порт. Поддръжка на Weighted Tail Drop (WTD) или еквивалентен алгоритъм за управление на задръствания. Поддръжка на Weighted Random Early Detection (WRED) или еквивалентен алгоритъм за предотвратяване на задръствания. DSCP и 802.1p маркиране на трафика на база трафични политики.
REQ. 34.	Протоколи и функции за управление и наблюдение: Web GUI.

	CLI. DNS. TFTP. FTP. NTP. SSHv2 и SNMPv3. Експортиране на трафична информация за 16000 трафични потока чрез IPFIX, NetFlow, JFlow или еквивалентен протокол към външна система за трафичен анализ. Вграден DHCP сървър. Задаване ниво на достъп до системата за всеки администратор. Traffic policing за контролиране на трафика до контролната система на комутатора. Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. Отделен Ethernet порт за out of band управление и наблюдение. API интерфейс с поддръжка на GNMI, RESTCONF и NETCONF. YANG дейта модели.
REQ. 35.	Комплект планки за монтаж в 19“ шкаф, стеков кабел, два захранващи кабела
Гаранция и поддръжка:	
REQ. 36.	Хардуерна гаранция за срок от минимум 3 (три) години.
REQ. 37.	Техническа поддръжка за срок от минимум 3 (три) години.
REQ. 38.	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.
REQ. 39.	Лицензни абонаменти за използване на софтуерни функции за срок от минимум 3 (три) години.

5. Комутатори за достъп – тип 2

Спецификация – минимални изисквания	
REQ. 1.	Количество – 9 броя.
REQ. 2.	Монтаж - в 19“ шкаф.
REQ. 3.	Токозахранване – модулно, с два токозахранващи модула, AC.
REQ. 4.	24 порта 1GE RJ45 с поддръжка на PoE+ и 4 порта 10GE SFP модули.
REQ. 5.	Вграден хардуерен порт за стеково свързване с производителност 80Gbps.
REQ. 6.	Изграждане на стек от 8 комутатора.
REQ. 7.	Брой USB портове – 1.
REQ. 8.	Сериен конзолен порт – 1.
REQ. 9.	Изолиране на потребителите от един и същ VLAN.
REQ. 10.	Идентификация и оторизация на достъпа: 802.1x идентификация и оторизация с прилагането на динамични VLAN и ACL. MAC authentication bypass.

	Идентификация чрез вграден Web портал. Комбиниране на методите за идентификация на един порт – 802.1x, MAC адрес, WEB идентификация. RADIUS CoA. 802.1x идентификация на повече от едно устройство на комутаторен порт. 802.1x Multi-Domain идентификация.
REQ. 11.	Хардуерно реализирани листи за филтриране на трафика, на база source/destination IP адреси, source/destination MAC адреси, протоколи и Layer 4 TCP/UDP номера на портове.
REQ. 12.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимален брой пакети в секунда
REQ. 13.	Storm control защита от broadcast, multicast и unicast трафик със задаване на максимална скорост в секунда.
REQ. 14.	802.1AE с 128 битово криптиране, с MKA.
REQ. 15.	DHCP Snooping или еквивалентен метод.
REQ. 16.	DHCP опция 82.
REQ. 17.	Dynamic ARP inspection или еквивалентен метод.
REQ. 18.	IP source guard или еквивалентен метод за защита от IP spoofing в мрежи с динамично и статично присвояване на IP адресите.
REQ. 19.	Автоматично запаметяване на използвания от първото клиентското у-во MAC адрес и блокиране на мрежовия достъп за други устройства, които се свързват към същия порт.
REQ. 20.	Spanning Tree защити - BPDU Guard и Root Guard.
REQ. 21.	Хардуерен модул за удостоверяване автентичността на хардуерна и софтуера чрез използване на криптографски методи.
REQ. 22.	Хардуерно IP forwarding и комутиране със следните параметри: Производителност – 175 Gbps. Forwarding – 130 Mpps. MAC адреси – 16000. IPv4 маршрути – 3000. Multicast маршрути – 1000. SVI интерфейси – 512. Пакетни буфери – 6MB.
REQ. 23.	DRAM - 2GB.
REQ. 24.	Statefull Switch Over (SSO) между комутатори в един стек за следните функции: Рутиране. STP. 802.3ad.
REQ. 25.	Jumbo frames - 9100 байта.
REQ. 26.	Spanning Tree – IEEE 802.1d, 802.1w и 802.1s.
REQ. 27.	Функция Private VLAN.

REQ. 28.	Разпознаване на мрежова връзка с еднопосочна пропускливост между два комутатора от същия вид.
REQ. 29.	Рутинг протоколи: RIP OSPF с 1000 маршрута. Мултикас рутиране с PIM. Рутиране на база политики. VRRP
REQ. 30.	IEEE 802.3ad LACP протокол.
REQ. 31.	IEEE 802.3ad групи с портове от различни комутатори в един стек.
REQ. 32.	IEEE 802.1AB (LLDP) и LLDP-MED.
REQ. 33.	QoS със следните функции, като минимум: HQoS. 8 изходящи пакетни опашки на всеки порт. Групиране на трафика в трафични класове на база Layer2, Layer 3 и Layer 4 трафични параметри, 802.1p и DCSP маркировка. Traffic policing. Traffic policing за входящ и изходящ трафик с възможност за задаване на CIR PIR и burst параметри. Traffic shaping. Управление на пакетните опашки чрез задаване на минимално гарантирана пропускателна способност за всеки клас от общата пропускателна способност на интерфейса. Поддръжка на две приоритетни опашки (PQ) на порт. Поддръжка на Weighted Tail Drop (WTD) или еквивалентен алгоритъм за управление на задръствания. Поддръжка на Weighted Random Early Detection (WRED) или еквивалентен алгоритъм за предотвратяване на задръствания. DSCP и 802.1p маркиране на трафика на база трафични политики.
REQ. 34.	Протоколи и функции за управление и наблюдение: Web GUI. CLI. DNS. TFTP. FTP. NTP. SSHv2 и SNMPv3. Експортиране на трафична информация за 16000 трафични потока чрез IPFIX, NetFlow, JFlow или еквивалентен протокол към външна система за трафичен анализ. Вграден DHCP сървър. Задаване ниво на достъп до системата за всеки администратор. Traffic policing за контролиране на трафика до контролната система на комутатора. Идентификация на администраторите чрез външни RADIUS и TACACS+ системи. Отделен Ethernet порт за out of band управление и наблюдение. API интерфейс с поддръжка на GNMI, RESTCONF и NETCONF.

	YANG дейта модели.
REQ. 35.	Комплект планки за монтаж в 19“ шкаф, стеков кабел, два захранващи кабела
Гаранция и поддръжка:	
REQ. 36.	Хардуерна гаранция за срок от минимум 3 (три) години.
REQ. 37.	Техническа поддръжка за срок от минимум 3 (три) години.
REQ. 38.	Получаване на нови версии на софтуера за срок от минимум 3 (три) години.
REQ. 39.	Лицензни абонаменти за използване на софтуерни функции за срок от минимум 3 (три) години.

5. Точки за безжичен достъп

Спецификация – минимални изисквания	
REQ. 1.	Количество – 6 броя
REQ. 2.	Монтаж – върху окачен таван.
REQ. 3.	Захранване – 802.3at PoE+ с консумирана мощност не по голяма от 26W.
REQ. 4.	Един IEEE 802.3bz интерфейс, който поддържа 1GE и 2.5GE.
REQ. 5.	Радио диапазони – 2.4GHz и 5GHz.
REQ. 6.	IEEE 802.11a/b/g/n/ac/ax и широчина на каналите 20, 40, 80 и 160MHz за 5GHz радио диапазон.
REQ. 7.	Data rate (2.4GHz и 5GHz комбинирано) – минимум 5Gbps.
REQ. 8.	Външна антенна система с усилване от 5 dBi за 5 GHz.
REQ. 9.	802.11ac и 802.11ax beamforming.
REQ. 10.	MRC за 802.11n, 802.11ac и 802.11ax.
REQ. 11.	BSS Coloring.
REQ. 12.	OFDMA за приемане и предаване.
REQ. 13.	Target Wake Time.
REQ. 14.	802.11ax и 802.11ac MU-MIMO.
REQ. 15.	Пакетна агрегация A-MPDU и A-MSDU.
REQ. 16.	4x4 MU-MIMO с 4 стрийма за 802.11ac и 802.11ax.
REQ. 17.	IEEE 802.11h.
REQ. 18.	IEEE 802.11d.
REQ. 19.	WPA2 и WPA3.
REQ. 20.	802.11i, AES шифроване
REQ. 21.	802.1X.

REQ. 22.	EAP методи – TLS, TTLS, PEAP, MS-CHAPv2, GTC, SIM.
REQ. 23.	Удостоверяване на софтуерната автентичност с криптографски методи -Secure Boot или еквивалентна технология.
REQ. 24.	Управление на всички функции и радио параметри чрез централен мрежови контролер.
REQ. 25.	Вграден Bluetooth 5.0 за реализиране на beacon функции.
REQ. 26.	Сериен конзолен порт.
REQ. 27.	2GB DRAM и 1GB flash
REQ. 28.	USB порт.
Гаранция и поддръжка	
REQ. 29.	Хардуерна гаранция за срок от мин. 3 (три) години.
REQ. 30.	Техническа поддръжка за срок от мин. 3 (три) години.
REQ. 31.	Предоставяне на нови версии на софтуера за срок от мин. 3 (три) години.
REQ. 32.	Лицензни абонаменти за използване на софтуерни функции за срок от мин. 3 (три) години.

6. Софтуерен контролер за управление на безжичните точки

Спецификация – минимални изисквания	
REQ. 1.	Софтуерен wireless контрол с възможност за виртуализация върху VMware ESXi средата на възложителя.
REQ. 2.	Вид – виртуален сървърен аплайънс за VMWare ESXi.
REQ. 3.	Пропускателна способност – 5Gbps.
REQ. 4.	Брой поддържани AP- 1000.
REQ. 5.	Брой поддържани клиенти - 10000.
REQ. 6.	Поддържани VLAN – 4000.
REQ. 7.	Управление на WiFi access point в това задание.
REQ. 8.	Обединяване на два контролера в HA клъстер със Stateful Switch Over.
REQ. 9.	Поддържане на 802.11b, 802.11g, 802.11a, 802.11n, 802.11ac и 802.11ax стандарти.
REQ. 10.	Системно подпомаган роуминг съгласно IEEE 802.11r с поддръжка на 802.11k и 802.11v.
REQ. 11.	802.11h.
REQ. 12.	802.11d.
REQ. 13.	QoS в WiFi средата съгласно 802.11e (WMM).

REQ. 14.	Автоматично управление на предавателната мощност и използваните радиоканали от точките за безжичен достъп, за постигане на оптимално покритие при променяща се радио среда.
REQ. 15.	Разпознаване на външни точки за достъп и клиенти – rouge AP и rouge clients.
REQ. 16.	Автоматично преместване на dual band клиенти към 5GHz.
REQ. 17.	Балансирано разпределение на клиентите между WiFi точките за достъп.
REQ. 18.	Локално 802.1Q бриджиране на трафика в WiFi AP, за всяка радиомрежа.
REQ. 19.	Централно 802.1Q бриджиране на трафика в контролера, за всяка радиомрежа.
REQ. 20.	Гарантирано доставяне на multicast трафика до безжичните клиенти чрез мултикаст към уникаст транслация.
REQ. 21.	Radius Override – използване на различни VLAN мрежи за клиенти, които са свързани към една и съща WLAN, на база Radius атрибут.
REQ. 22.	Класифициране на трафика в трафични класове.
REQ. 23.	Двупосочен rate limit.
REQ. 24.	Филтриране и rate-limiting на трафика на ниво SSID.
REQ. 25.	Филтриране и rate-limiting на трафика на ниво клиент.
REQ. 26.	Разпределяне на времето за достъп до радио средата между различните WLAN в downstream посока.
REQ. 27.	Управление на WiFi MESH система чрез съвместими WiFi AP.
REQ. 28.	Поддръжка на Hotspot 2.0.
REQ. 29.	Поддръжка на WiFi 6 клиенти.
REQ. 30.	802.1x идентификация чрез външен RADIUS и Radius DTLS сървъри.
REQ. 31.	MAC authentication bypass -MAB.
REQ. 32.	Поддръжка на 802.11w.
REQ. 33.	Филтриране на трафика на ниво адреси и номера на портове чрез използване на листи за достъп (ACL).
REQ. 34.	Поддръжка на DNS базирани листи за контрол на достъпа.
REQ. 35.	Идентификация на потребителите чрез LDAP и Secure LDAP интеграция с външна директория.
REQ. 36.	EAP методи за локална идентификация – TLS и PEAP.
REQ. 37.	Поддръжка на WPA2 и WPA3.
REQ. 38.	Поддръжка на WPA3 SAE Hash-to-Element.
REQ. 39.	Вграден Web портал за идентификация с потребителско име и парола.
REQ. 40.	Поддръжка на MAC Authentication Bypass.
REQ. 41.	Отклоняване на Web сесия към външни портали за идентификация на потребители.
REQ. 42.	Динамични VLAN and ACL за всеки потребител на база Radius атрибути.
REQ. 43.	Използване на няколко PSK в една радио мрежа.

REQ. 44.	GUI WEB интерфейс.
REQ. 45.	DHCP клиент.
REQ. 46.	DHCP опция 82.
REQ. 47.	Вградени DHCP сървъри за Wi-Fi клиентите.
REQ. 48.	Ъпгрейд на свързаните WiFi AP.
REQ. 49.	DNS.
REQ. 50.	TFTP.
REQ. 51.	SNTP.
REQ. 52.	SSH, SNMPv2 и v3.
REQ. 53.	Syslog.
REQ. 54.	Експортиране на трафична информация чрез jFlow, NetFlow, sFlow, IPFIX или еквивалентен протокол към външна система за трафичен анализ.
REQ. 55.	Идентификация на администраторите чрез локална база и външен RADIUS сървър.
REQ. 56.	Шифроване на контролните връзки между контролера и WiFI AP с DTLS или еквивалентен метод.
REQ. 57.	NETCONF-YANG интерфейс.
Гаранция и поддръжка	
REQ. 58.	Техническа поддръжка за срок от мин. 3 (три) години.
REQ. 59.	Получаване на нови версии на софтуера за срок от мин. 3 (три) години.
REQ. 60.	Лицензни абонаменти за използване на софтуерни функции за срок от мин. 3 (три) години.

7. **Кабели**

Техническа спецификация	
REQ.1	Количество – 4 броя.
REQ.2	10GE оптичен DAC кабел с дължина 3м и SFP+ интерфейси.
REQ.3	Кабелът трябва да бъде от същия производител, както предложените комутатори, или да бъде сертифициран за използване от него.

8. **Интерфейсни модули**

Техническа спецификация	
REQ.1	Количество – 40 броя.
REQ.2	10GBASE-SR SFP+ модул.
REQ.3	Конектор – дуплексен LC.
REQ.4	Модулът трябва да бъде от същия производител, както предложените комутатори, или да бъде сертифициран за използване от него.

9. **Инсталация и въвеждане в експлоатация**

Изпълнението на заявката обхваща допълнителни дейности по инсталация, конфигурация и въвеждане в експлоатация на доставеното оборудване и софтуер по т. 1 до т. 8 включително. Ще бъде подписан приемо-предавателен протокол удостоверяващ извършената инсталация и въвеждане в експлоатация на доставеното оборудване и софтуер.

II. ИЗИСКВАНИЯ КЪМ ИЗПЪЛНЕНИЕТО НА ЗАЯВКАТА

1) Заявки за обслужване (тикети) за доставения хардуер се подават чрез осигурена от Изпълнителя онлайн система за управление на заявки (СУЗ). Всички заявки, получени чрез електронна поща или телефон следва да бъдат регистрирани в СУЗ.
2) Оборудването, предмет на доставката, трябва да бъде фабрично ново, неупотребявано, да е в актуалните продуктови листи на производителя и да не е спряно от производство.
3) Хардуерните компоненти на оборудването трябва да отговарят на всички стандарти в Република България относно ергономичност, пожарна безопасност, норми за безопасност и включване към електрическата мрежа.
4) Хардуерът следва да бъде доставен в пълно работно състояние, в оригиналната опаковка на производителя с ненарушена цялост, окомплектовано с всички необходими интерфейсни и захранващи кабели, където се изискват, както и с необходимата техническа документация (на електронен носител или чрез линкове, от които може да бъде свалена).
5) В случай че не е производител, доставчикът следва да е надлежно оторизиран от производителя или негов официален представител за правото на разпространение/доставка и предоставяне на гаранционна поддръжка на предлаганите софтуерни и хардуерни продукти на територията на Република България.

III. СРОК НА ИЗПЪЛНЕНИЕ. УСЛОВИЯ НА ДОСТАВКА

Доставката на оборудването се извършва в срок до 31.12.2024 г.

IV. МЯСТО НА ДОСТАВКА И ГАРАНЦИОННО ОБСЛУЖВАНЕ

1) Мястото на извършване на доставката е сградата на Министерство на енергетиката, намираща се в гр. София, ул. 1000, ул. "Триадица" 8
2) Гаранционното обслужване ще се извършва спрямо местонахождението на инсталираното оборудване.

V. ГАРАНЦИЯ И ПОДДРЪЖКА. УСЛОВИЯ НА ГАРАНЦИОННО ОБСЛУЖВАНЕ

1) Доставчикът гарантира пълната функционална годност на доставеното оборудване, съгласно предписанията на производителя.
2) В съответствие с режима на гаранционно обслужване доставчикът отстранява за своя сметка всички повреди и/или несъответствия на оборудването, съответно подменя дефектирали части, устройства, модули и/или компоненти с нови съгласно предписанията на производителя. В гаранционното обслужване се включва замяна на част (компонент) със скрити недостатъци с нова или на цялото устройство с ново, ако недостатъкът го прави негодно за използване по предназначението му, както и всички разходи по замяната.
3) Времето за реакция е до 8 часа от уведомяването му.
   * Време за реакция е времето от момента на уведомяване от страна на Възложителя за възникнал проблем до обратна реакция (обаждане или пристигане на място) от доставчика.
4) Доставчикът е длъжен да осигури преглед на място в срок не по-късно от следващия работен ден.
5) Доставчикът се задължава да отстрани настъпилата повреда и/или несъответствие и възстановяване на пълната работоспособност на оборудването. Отстраняването на настъпила повреда и/или несъответствието се осъществява по местонахождение на оборудването до 72 часа от установяването.
6) В случай, че повредата и/или несъответствието прави устройството негодно за използване по предназначението му, доставчикът е длъжен да го замени с ново, с параметри, гарантиращи същата или по-добра функционалност и производителност.
7) За всяка извършена замяна на оборудване в рамките на гаранционното обслужване, доставчикът изготвя и предоставя протокол, който съдържа описание на новото и замененото оборудване. Протоколът се подписва от представители на двете страни.
8) Всички разходи по време на гаранционното обслужване са за сметка на изпълнителя.

VI. ИЗИСКВАНИЯ КЪМ МРЕЖОВАТА И ИНФОРМАЦИОННАТА СИГУРНОСТ[1]

1. Изпълнителят следва да осигури прилагането на изискванията на Закона за електронното управление, Закона за защита на личните данни, Закона за киберсигурност и подзаконовите нормативни актове към тях.

2. Във връзка с мрежовата и информационната сигурност на Възложителя/МЕ и в съответствие с чл. 10 от Наредбата за минималните изисквания за мрежова и информационна сигурност (НМИМИС), Изпълнителят:

   1) Гарантира, че лицата, ангажирани от Изпълнителя с изпълнението на Услугата (в т.ч. подизпълнители, когато е приложимо) и които ще имат достъп до информация и активи, при взаимодействието им със служители на Възложителя/МЕ ще спазват изискванията за сигурността на информацията съгласно Закона за киберсигурност и НМИМИС.
   2) При предоставяне на Услугата спазва правилата за сигурността на информацията на Възложителя/МЕ. За целта, непосредствено преди началото на изпълнение, ангажираните от Изпълнителя за предоставяне на Услугата лица (в т.ч. и подизпълнителите, когато е приложимо), които ще имат достъп до информация и активи на

Възложителя/МЕ, подписват декларации по образец на Възложителя за опазване на информацията, които се предават на Възложителя. При промяна на лицата в хода на изпълнението съответните подписани декларации се предават, в срок до 2 (два) работни дни от промяната.

3) Определя компетентното лице, отговорно за мрежовата и информационна сигурност, което осъществява взаимодействие с компетентно лице от страна на Възложителя при възникване на инцидент по МИС;
4) Осигурява адекватни и комплексни мерки за защита за мрежова и информационна сигурност, основани на извършения анализ и оценка на риска, с цел да се гарантира необходимото ниво на сигурност. Имплементираните смекчаващи механизми трябва да са пропорционални на рисковете, в частност на щетите, които те биха могли да нанесат.

3. Изпълнителят се задължава да не разпространява информация, станала му известна при и по повод изпълнението на Услугата на трети страни без изричното писмено съгласие на Възложителя/ МЕ.

4. При неспазване на изискванията за сигурност на информацията Изпълнителят дължи неустойка съгласно уговореното в договора.

5. Лицата, отговорни за мрежовата и информационната сигурност и параметрите на нивото на обслужване при изпълнение на Договора („лица по чл. 10, ал. 2 от НМИМИС“) имат следните права и задължения:

1. При изпълнението на задълженията си, осъществяват комуникация с лицата, които ще имат достъп до системите на МЕ;

2. Лицето по чл. 10, ал. 2 от НМИМИС от страна на Изпълнителя отговаря за прилагането на адекватни мерки за мрежова и информационна сигурност от страна на Изпълнителя (и на подизпълнителите, когато е приложимо);

3. При получена информация, лица по чл. 10, ал. 2 от НМИМИС осъществяват незабавна комуникация по телефон и/или имейл и предприемат действия за извършване на анализ на: причините за влошаване на качеството по отношение на времената за реакция и за възстановяването на работата; условията, при които инцидентът може да бъде затворен; рискът за постигане на целите на мрежовата и информационната сигурност на Възложителя/МЕ;

4. При констатирано неспазване на изискванията за сигурност на информацията или неспазване на договорените срокове, количество и/или качество на услугата, което може да създаде риск за мрежовата и информационната сигурност за Възложителя/МЕ, лицата по чл. 10, ал. 2 от НМИМИС съвместно с лицата, които ще имат достъп до системите на МЕ от страна на Възложителя и на Изпълнителя извършват анализ и набелязват мерки за отстраняване на допуснатата нередност в определен срок.